



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,801	05/15/2006	Yong Ding	25515-0002	3452
29052 7590 12/18/2007 SUTHERLAND ASBILL & BRENNAN LLP 999 PEACHTREE STREET, N.E. ATLANTA, GA 30309				
			EXAMINER LE, CANH	
			ART UNIT 2139	PAPER NUMBER
			MAIL DATE 12/18/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/579,801

Applicant(s)

DING ET AL.

Examiner

Canh Le

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4 and 8-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 8-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Office Action is in response to the application filed on 10/23/2007.

Claims 5-7 have been cancelled.

Claims 1-2, 4, 11, 13-16 have been amended.

Claims 1-4 and 8-16 are pending and have been examined.

Response to Arguments

Applicant's arguments filed 10/23/2007 have been fully considered but they are not persuasive.

With regard to claim 1-4 and 13-14, The Applicant argues that:

"Independent Claim 1 provides for digital signature schemes based on braid group conjugacy. Compared with the digital signature method provided by the cited reference cited in the Office Action, a distinguishing feature of Claim 1 is as follows: in the digital signature scheme provided by Claim 1, the braid group $B_n(l)$ is divided into a left subgroup $LB_m(l)$ and a right subgroup $RB_{n-l-m}(l)$, and in Step 3, a random braid b is generated in the right subgroup $RB_{n-l-m}(l)$ of the braid group based on the exchangeability of the left and right subgroups (see the related description in the specification, page 2, paragraph [0049] of Publication No. 2007/0104322A1); while the digital signature method disclosed in the cited reference (section 2.3 on page 4-5) does not involve the concepts that the braid group is divided into a left subgroup and a right subgroup, and the random braid b is generated within the whole braid group".

The Examiner respectfully disagrees that:

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "the braid group is divided into a left subgroup and a right subgroup") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Dependent claims 2-4 and 13-14 which depend from independent claim 1. See further rejections below.

With regard to claim 8-12 and 15-16, The Applicant mentions that:

"Independent Claim 8, which recites similar patentable features as independent Claim 1".

Claim 8 recites similar features as independent claim 1. Please, see the same argument as claim 1.

Dependent claims 9-12 and 15-16 which depend from independent claim 8. See further rejections below.

Therefore, the Examiner asserts that cited prior does teach or suggest the subject matter recited claims 1-4 and 8-15.

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative should not be construed as indicating Examiner's agreement therewith.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 and 13-14 are rejected under 35 U.S.C. 102(b) as being anticipated by K.H. Ko et al., "New Signature Scheme Using Conjugacy Problem", November 11, 2002, pages 1-13.

As per claim 1:

Ko teaches a digital signature scheme based on braid group conjugacy problem, parameters involved in this scheme comprising a signatory S, a signature verifying party V, a message M needing signature, an integer n for a number of generators in the braid group, an integer m for the number of generators in a left subgroup, an integer l for an upper bound of the length of a braid, a braid group $B_{sub.n(l)}$, a left subgroup $LB_{sub.m(l)}$ of $B_{sub.n(l)}$, a right subgroup $RB_{sub.n-1-m(l)}$ of $B_{sub.n(l)}$, a one way

hash function h from bit sequence $\{0,1\}^*$ to braid groups $B_{\text{sub}.n(l)}$; said signature scheme comprising the following steps of:

(a) Step 1. A signatory (S) selecting three braids $x_{\text{epsilon}.LB.\text{sub}.m(l)}$, $x'_{\text{epsilon}.B.\text{sub}.n(l)}$, $a_{\text{epsilon}.B.\text{sub}.n(l)}$, and making them meet $x'=a.\text{sup}^{-1}xa$, moreover, with known x and x' , it being impossible to find a in calculation, and considering braid pair (x',x) as a public key of signatory (S), braid a as a private key of signatory (S) [pg. 4-5; section 2.3 Description of conjugacy signature scheme section; “Key generation ...on the braid groups”];

(b) Step 2. signatory (S) using hash function h for message (M) needing signature to get $y=h(M)_{\text{epsilon}.B.\text{sub}.n(l)}$ [pg. 4-5; section 2.3 Description of conjugacy signature scheme section; “Signing: Given a message m , a signature ... on the braid groups”];

(c) Step 3. generating a braid $b_{\text{epsilon}.RB.\text{sub}.n-1-m(l)}$ at random, then signing the message (M) with the own private key a and a generated random braid b to obtain $\text{Sign}(M)=a.\text{sup}^{-1}byb.\text{sup}^{-1}a$; and

(d) Step 4. the signatory (S) outputting message (M) and a signature of message (M) $\text{Sign}(M)$ [pg. 4-5; section 2.3 Description of conjugacy signature scheme section].

As per claim 2:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein generating the public key braid pair (x', x) and the private key braid a of signatory (S) in said step 1 comprises the following steps of:

(a) Step 1a. selecting a distance d between system parameter braid groups public key pairs [pg. 9-10; 4.1 Random braids and braid signature scheme; “the distance $d(x, y)$ between x and y is defined by ... Return accept if and only if”].

(b) Step 1b. representing x into a left canonical form $x = \Delta^{\pi_1} \pi_2 \dots \pi_n$ [pg. 5-6; 3.1 Brief introduction to braid group section; “We introduce necessary ... This unique decomposition of a braid b is called a left canonical form... in a high probability”];

(c) Step 1c. selecting a braid b at random to belong to a set $B_n(5l)$ [pg. 5-6; 3.1 Brief introduction to braid group section; pg. 9-10; 4.1 Random braids and braid signature scheme section; “We first choose b belong to set $B_n(5l)$ if $l(x)=l$... Return accept if and only if”];

(d) Step 1d. calculating $x^{\sup} = \sup_{-1} x b, a = b$ [pg. 6-7; 3.2 Conjugator search problem in Braid groups section; pg. 9-10; 4.1 Random braids and braid signature scheme section; “We first choose b belong to set $B_n(5l)$ if $l(x)=l$. Then we apply a random sequence of cyclings and decyclings to ... Return accept if and only if”];

(e) Step 1e. generating a bit at random, if 1, calculating $x^{\sup} = \text{decycling}(x^{\sup})$, $a = \pi_1$; if not 1, calculating $x^{\sup} = \text{cycling}(x^{\sup})$, $a = \tau^{\sup}(\pi_1)$ [pg. 6-7; 3.2 Conjugator search problem in Braid groups

section; "There are two useful conjugations of a braid ...The cycling on x is given by ... and the decycling on x ... level for MCSP as well"; pg. 9-10; 4.1 Random braids and braid signature scheme section ; "We first choose b belong to set $B_n(5l)$ if $l(x)=l$. Then we apply a random sequence of cyclings and decyclings to ...Return accept if and only if";

(f) Step 1f. judging whether $x.\text{sup.}'$ belongs to $SSS(x)$ and whether $l(x.\text{sup.}').l \leq d$, if all the conditions are yes, outputting the braid pair $(x, x.\text{sup.}')$ as the public key, a as the private key; if either of them is not, performing step 1e [pg. 6-7; 3.2 Conjugator search problem in Braid groups section; "Super Summit Set We now discuss a mathematical solution The super summit set $SSS(x)$ of s is defined byThere are two useful conjugations of a braidThe cycling on x is given by and the decycling on x ... level for MCSP as well"; pg. 9-10 Random braids and braid signature scheme section].

As per claim 3:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein the process for obtaining $y=h(M).\epsilon.B.\text{sub}.n(l)$ by using the hash function h in said step 2 comprises the following steps of:

(a) Step 2a, selecting an ordinary hash function H , with a length of output $H(M)$ is $l[\log(2,n!)]$, then dividing $H(M)$ into l sections $R.\text{sub}.1.\text{parallel}.R.\text{sub}.2.\text{parallel} \dots$

.parallel.R.sub.1 in equal at one time [pg. 9-10; 4.1 Random braids and braid signature scheme section].

(b) Step 2b, corresponding R_i to a permutation braid A_i , then calculating $h(M)=A_1*A_2 \dots A_l$, that is the $h(M)$ required [pg. 9; 4.1 Random braids and braid signature scheme section].

As per claim 4:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein a integer n for the number of generators in a braid group is in the range of 20.about.28, an upper value of the braid length is $l=3$, $d=4$, and an left subgroup $n-m=4$ [pg. 11-12; 4.3 Parameters suggestion and performance section; 4.4 Performance table section].

As per claim 13:

Claim 13 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 14:

Claim 14 is essentially the same as claim 4 and rejected under the same reasons as applied above.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 8-12 and 15-16 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over K.H. Ko et al., "New Signature Scheme Using Conjugacy Problem", November 11, 2002, pages 1-13.

As per claim 8:

Claim 8 is essentially the same as claims 1 for step 1-4 rejected under the same reasons as applied above with additional following steps:

(a) Step 5. a signature verifying party (V) obtaining a public key of a signatory (S) after receiving a message (M) and its signature $\text{Sign}(M)$ transmitted from the signatory (S) [pg. 4-5, **2.3 Description of conjugacy signature scheme section**];

(b) Step 6. calculating the message M by employing a system parameter hash function h, and obtaining $y=h(M)$ [pg. 4, **2.3 Description of conjugacy signature scheme; "Signing: Given a message m, ... for $y = h(m)$ "**];

(c) Step 7. judging whether $\text{sign}(M)$ and y are conjugate or not, if not, $\text{sign}(M)$ is an illegal signature, and the verification fails; if yes, perform step 8 [pg. 4-5; **2.3 Description of conjugacy signature scheme; "Verifying: A signature ...implement**

it on the braid groups”; pg. 7; 3.3 Conjugacy decision algorithm in braid group (BCDA) to pg. 10; “ Verifying Algorithm: $\text{Ver}(\text{pk}, \text{m}, \text{sigma}) = \{\text{accept}|\text{reject}\}$ ”; and

(d) Step 8. calculating $\text{sign}(\text{M}) \times'$ and xy by using the public key of obtained S , and judging whether they are conjugate or not, if not, $\text{sign}(\text{M})$ is an illegal signature, the verification fails; if yes, $\text{sign}(\text{M})$ is the legal signature of message (M) [pg. 4-5; 2.3

Description of conjugacy signature scheme; “ Verifying: A signature ...implement it on the braid groups”; pg. 7; 3.3 Conjugacy decision algorithm in braid group (BCDA) to pg. 10; “ Verifying Algorithm: $\text{Ver}(\text{pk}, \text{m}, \text{sigma}) = \{\text{accept}|\text{reject}\}$ ”].

As per claim 9:

Claim 9 is essentially the same as claim 2 and rejected under the same reasons as applied above.

As per claim 10:

Claim 10 is essentially the same as claim 3 and rejected under the same reasons as applied above.

As per claim 11:

Claim 10 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 12:

Ko further teaches the digital signature scheme based on braid group conjugacy problem and a verifying method thereof according to claim 8, wherein algorithm BCDA is employed in judging whether $\text{sign}(M)$ and y are conjugate or not in step 7 and judging whether $\text{sign}(M) x'$ and xy are conjugate or not in step 8 [pg. 7-8; 3.3 Conjugacy decision algorithm in braid groups (BCDA) section].

As per claim 15:

Claim 15 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 16:

Claim 16 is essentially the same as claim 4 and rejected under the same reasons as applied above.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

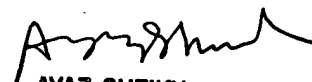
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

Application/Control Number:
10/579,801
Art Unit: 2139

December 13, 2007

Page 13



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100